INTER PLANT STANDARD – STEEL INDUSTRY		
IPSS	**GUIDELINES FOR DATA EXCHANGE AND REMOTE ACCESS ACROSS SERVER**	**IPSS:2-08-03-13**

0. FOREWORD

0.1. This interplant standard has been prepared by the standards committee on Information & Communication Technology, IPSS 2:8, with the active participation of the representatives of the steel plants, major consulting organizations and established manufacturer and was adopted in June, 2013.

0.2. Steel Industry has taken rapid strides in leveraging IT for making its business process agile and responsive. It has rolled out various IT applications covering most of the business process. It is important requirement to define the norms to use the Data Exchange and Remote Access to Server in a secured manner.

1. SCOPE

1.1. The purpose of these guidelines are to define the norms to use the Data Exchange and Remote Access to Server in a secured manner.

1.2. The objective of these guidelines are to have greater Operational Controls and reduce the risk of harmful unauthorised access of the system.

1.3. This policy is applicable to all Servers being used for providing various services.

2. GUIDELINES & PROCEDURE

2.1. DeactivateTelnet Service in the reverse proxy system through which internet users are allowed to access the Servers

2.2. SFTP (Secure File Transfer Protocol) or WinSCP (Windows Secure Copy), or other secured Protocol may be used for file transfer between two Servers within intranet.

2.3. SSH may be used instead of unsecured Telnet service.

2.4. For UNIX/LINUX Systems “Chroot Jailed FTP” is a better solution, which restricts the FTP user to a particular directory for which the access is given. The user cannot browse other directories/folders. The FTP user should not be given access to any other services except the file transfer.

3. RESPONSIBILITY

For responsibility & definition of Asset Owner and the system administrator, refer IPSS Standard **IPSS: 2-08-02-13**